LA-10804-SR
Status Report

Department of Energy

CENTER FOR COMPUTER SECURITY

FY 1986
Activities and Accomplishments of the DOE Center for Computer Security

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36.

Los Alamos
Los Alamos National Laboratory
Los Alamos, New Mexico 87545

This work was supported by the U.S. Department of Energy, Office of Safeguards and Security.

Prepared by Sharon Hurdle, Group Q-4

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

LA-10804-SR
Status Report

UC-32
Issued: October 1986

FY 1986 Activities and Accomplishments of the DOE Center for Computer Security

Compiled by
R. B. Strittmatter

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

FY 1986 ACTIVITIES AND ACCOMPLISHMENTS OF THE DOE CENTER FOR COMPUTER SECURITY

Compiled by

R. B. Strittmatter

ABSTRACT

The Department of Energy (DOE) Center for Computer Security (CCS) at Los Alamos National Laboratory is responsible for developing, collecting, organizing, and disseminating computer security information to the DOE and DOE contractors. This responsibility involves operations and field support, computer security education and awareness, and research and development. During the current fiscal year, the Center completed the Link ACE II, the DOE/CCS computer laboratory and Wide-Band Security Test Bed, and the computer security products database and its merger with the National Bureau of Standard's database. Also completed was the implementation of the Data Encryption Standard on the Wide-Band Communications Network.

I. INTRODUCTION

The Department of Energy Center for Computer Security (DOE/CCS) at Los Alamos National Laboratory is responsible for developing, collecting, organizing, and disseminating computer security information to the DOE and DOE contractors. Fulfilling this responsibility involves operations and field support, computer security education and awareness, and research and development. Particular accomplishments of the Center for the current fiscal year included the completion of the computer security products database and its merger with the National Bureau of Standards (NBS) database, completion of the Link Access Control and Encryption (ACE) II, implementation of the Data Encryption Standard on the Wide-Band Communications Network (WBCN), and completion of the DOE/CCS computer laboratory and Wide-Band Security Test Bed (WBSTB). In addition, the Center has continued to provide to DOE/OSS Headquarters computer security expertise for the Inspection and Evaluation (I&E) Standards and Criteria Committee.

Technical contributors directly associated with the Center for Computer Security include A. L. Baker, L. H. Baker, S. Bogenholm, B. W. Burnham, W. Ford, J. F. Hafer, D. G. Harder, W. J. Hunteman, R. E. Lewis, T. G. Marr, D. P. Martinez, L. Massagli, C. J. McHale, J. R. Phillips, S. T. Smith, R. M. Tisinger, all of group Q-4; and T. M. Boorman and W. M. Robson, of group E-8.

The following individuals were not associated with the Center but contributed to activities described in this report: D. L. M. Irion, J. E. Coleman, W. T. Work, and K. E. Schommer, group OS-4; F. C. Jahoda and P. R. Foreman, group CTR-8; G. I. Chandler, group J-8; and J. J. Childers and J. P. Manning of the EG&G Los Alamos office.

Center accomplishments for this fiscal year are summarized below in the format of the Center's Tasking Statement.

II. OPERATIONS AND FIELD SUPPORT

A. Physical Center

Center personnel were moved to a central location where many of the CCS resources will also be concentrated. This move into two adjacent transportable buildings has provided secure space for the Center's VAX/750 secure computing system and office space for at least seven people. The relocation not only will improve the efficiency of the overall program operations but also will enhance the image of the CCS as a "center" of expertise in DOE computer security. The buildings are located within easy walking distance of the CCS laboratory building, which houses the WBSTB.

Engineering studies of physical, environmental, and security requirements of the computer system to be housed at the site were completed. The Laboratory Operational Security staff made preliminary assessments of physical security and electrical emanations. Their suggestions are being addressed in a draft security plan for the system that has been submitted to the Laboratory Computer and Telecommunications Security group for approval.

B. Newsletter

A quarterly newsletter, the "Center for Computer Security News," is published by the CCS to provide computer security education to computer systems security officers (CSSOs) and others interested in computer security. Recent issues reported on changes in DOE computer security management, the Ninth DOE Computer Security Group Conference, and issuance of DOE security guidelines and described computer security operations at various DOE sites. The newsletter has a circulation of about 800 readers throughout the DOE complex.

C. Participation in the DOE Computer Security Conference

The Ninth DOE Computer Security Group Conference was held May 6-9, 1986, in Las Vegas, Nevada. This annual conference provides DOE and DOE contractor personnel with a cost-effective forum for exchanging information on computer security. The Center planned, coordinated, and scheduled speakers; published and distributed the preconference proceedings; and managed registration. Three Center members contributed technical papers or presentations.

D. Interacting/Consulting with DOE Facilities

The CCS is continually interacting with DOE contractor personnel regarding current and anticipated site-specific issues and needs. These interactions provide a broad perspective on the current state of computer security in the DOE. This fiscal year, the CCS consulted with Sandia National Laboratories, Albuquerque, on a CRAY-XMP/CTSS security test and assessed computer security vulnerability at Pantex. Both activities were performed under separate contract to the Center.

E. Headquarters Assistance

Duane Harder was assigned as the Center liaison to Washington from May 1985 to May 1986. Alice Baker succeeded him for one year starting in June 1986.

The Center has contracted with BK Dynamics, Inc., for administrative, technical, and programmatic support. Although this support is available for all Center activities, it is principally for supporting the Center representative at Headquarters, and assignments to BK Dynamics are made by that person.

F. Product Database

The Center has compiled lists of computer security products and vendors for the DOE computer security community. These lists cover a wide range of commercial products designed to enhance the security of computer systems. Although the products were selected primarily for use with small systems, many can also be used with larger systems.

The Center obtained names of vendors from trade publications, publicly available databases, and advertisements in newspapers and magazines, as well as from personal contact with vendors. For every product listed, the vendor was the source of the data. No attempt was made to test items to verify performance, and their inclusion in this list does not constitute endorsement by the DOE. Each product is listed only once under a product type that most accurately represents its principal function.

The Center merged its DOE/CCS database with a similar product database developed by the NBS. The merged database was delivered to NBS where it will be maintained. As a result of this merger, vendors of 127 products not contained in the DOE database but listed in the NBS database were contacted. The DOE database contained 104 products not listed in the NBS database. The merged database contains approximately 400 products from about 250 vendors listed under 42 product-type categories.

III. EDUCATION AND AWARENESS

A. Education Planning and Development

In line with providing computer security education to the DOE community, the CCS developed a plan for a library of modules covering a wide range of computer security topics. With this library, educational activities can be tailored to the needs of the individual DOE facility or contractor, thus eliminating last-minute preparation of visual aids and presentation outlines. In addition, the "top-down" design approach allows for the modularization of the effort and the optimization of Center staff members' time.

We have contracted with BK Dynamics to develop a revised CSSO class. Course development by BK Dynamics will ensure timely availability of education for the DOE community while allowing optimum use of the remaining Center resources.

B. Computer Security Enhancement Reviews

Computer Security Enhancement Reviews (CSERs) are routinely conducted. In these informal, quick-check reviews, Center experts evaluate a computer security program for significant vulnerabilities and quality of program implementation. The CSERs are conducted in a nonthreatening mode; the results of the CSER are not documented outside the facility, nor are other organizations or persons briefed on the results.

This fiscal year, CSERs were conducted at

- Knolls Atomic Power Laboratory, November 5-8, 1985;
- Pantex, December 16-20, 1985; and
- Idaho National Engineering Laboratory, April 14-25, 1986.

C. Presentations

Another avenue of computer security education and awareness includes CCS presentations. Center staff made presentations to the Los Alamos office of EG&G and the EG&G/Energy Measurements group at NTS.

IV. RESEARCH AND DEVELOPMENT

A. Clyde Audit Software Appraisal

One of the current problems in computer security within the DOE community is to develop a system for auditing computer system activity. The Clyde Digital Systems (CDS) Company offers a product that performs an audit function in the VAX/VMS environment. A number of facilities knew of this product, and its suitability needed to be determined. The Center initiated a performance appraisal to discover and document for the DOE the extent of the audit available with this product, its robustness, and the ease with which the audit information can be managed. We negotiated with the CDS company concerning the appraisal of their software and drafted a performance appraisal description encompassing testing of the audit product on the recently completed DOE/CCS WBSTB. This draft description was circulated among technical staff of the Laboratory and the vendor. This activity was terminated because of CCS resource limitations.

B. Password Generator

We developed a specification for a password generator package. The specification incorporates the DOE requirements for passwords and the guidelines in the Department of Defense (DoD) Password Management Guideline issued by the National Computer Security Center (NCSC) (CSC-STD-002-85).

C. LAVA Development

We have been developing a methodology for performing automated vulnerability assessments on systems that are characterized by a set of safeguards protecting a set of assets from a set of threats. This methodology is called LAVA, an acronym for Los Alamos Vulnerability Assessment. LAVA is a qualitative/quantitative methodology based upon classical probability theory, decision theory, event-tree methods, fuzzy-set theory, utility theory, and hierarchical multilevel system theory.

The LAVA vulnerability assessment is performed by a team of in-house personnel. Median interactive time required for the assessment is 2 days. We know that a risk analysis performed by some consulting organizations has taken from 3 to 6 months and cost about $250K. In comparison with these figures, LAVA's performance looks very good indeed; furthermore, LAVA can be reused for as many analyses as are required.

Early in December 1985, 28 representatives of various government agencies attended at Los Alamos the first workshop and training class in LAVA. We used insights gained from the training workshop to restructure and reorganize the LAVA questionnaire. In addition, we reviewed the questionnaire to ensure it addressed the same issues as are addressed by the CSERs and the DOE Inspection and Evaluation reviews. As a result, we added 200 questions to the event-tree branches.

We established a LAVA development team to produce version 1.0 of LAVA for use in the field without extensive training and other support activities that were required in earlier versions. The development team defined the components for version 1.0, established the minimum hardware and software configuration, and prepared a project plan. According to the plan, version 1.0 will be delivered to DOE/OSS for review and comment by October 15, 1986, and distribution to the field will begin on November 12, 1986.

D. CSSO Tool Kit

The CCS is researching tools for improving the computer security program at individual systems or facilities. The tools will help administer computer security and standardize such areas as password generation and audit-trail analysis.

Programming specifications for a PC-based password generator and a file-integrity authenticator for IBM PCs have also been developed. We have integrated the inputs received from six operations offices and are developing a plan for the first phase of the CSSO tool kit. Suggested items include software packages to help in implementing computer security requirements, listings of computer security publications, listings of solutions to generic computer security problems in DOE, and security testing/certification guidelines.

E. Audit-Trail Analysis

We have developed a preliminary set of specifications for an automated audit-trail analysis package to enable a CSSO to detect abnormal log-in activity. Tentative plans are to investigate using an expert system developed for a safeguards application that interacts with the user to extend the inference rules thereby improving the definition of acceptable activity.

F. Secure Networks

1. LINK ACE. The Link ACE II was designed and developed by Los Alamos through the DOE/CCS. A pair of encryption units (one master, one remote) protects the transmission of unclassified sensitive data over data

links between central computers and remote terminals. These lines can be either dial-up or direct connections. They will also operate in a link where data from several terminals, PCs, or computers are multiplexed onto a communications line. With this flexibility, the Link ACE II units (Fig. 1) easily fit into existing networks. The unit consists of a printed circuit board containing encryption and communications logic, power supply circuitry, and tamper-detection circuitry. A secure lock box with pick-resistant locks encloses the unit.

The Link ACE II units were tested before shipment. A final project report describes the Link ACE II features and applications. Facilities and applications using the Link ACE II include Los Alamos National Laboratory, Nevada Badge System, Nuclear Regulatory Commission, Martin Marietta Energy Systems, Inc., and EG&G Kennedy Space Center-NASA. The Link ACE II technology has been transferred to RESDEL Engineering Corporation in Arcadia, California. RESDEL has a nonexclusive license from the DOE to manufacture and sell the Link ACE II encryption units.

2. Ungermann-Bass Network Security Analysis. The Ungermann-Bass Local Area Network (LAN) installed at Los Alamos has been expanded with additional ports to increase the usage of the network to aid in the evaluation. We exercised the security features of the test system to determine their characteristics and noted any anomalies for further investigation. Using this information, we presented a paper at the Ninth DOE Computer Security Conference. We are continuing our efforts to obtain the source code for the network software.

3. Measurement of Channel Isolation in a Broadband Local Area Network. The Albuquerque Operations Office of DOE (DOE-AL) is installing a broadband local area network (LAN). This network will provide convenient access to many of that office's computing resources. To minimize the cost of providing access to both secure and nonsecure computers, it is proposed that frequency-division multiplexing be used to provide multiple data-communications channels on the LAN. A consideration in deciding whether access to classified information can be permitted through this LAN is the degree of isolation that exists between the channels assigned to secure resources and other channels.

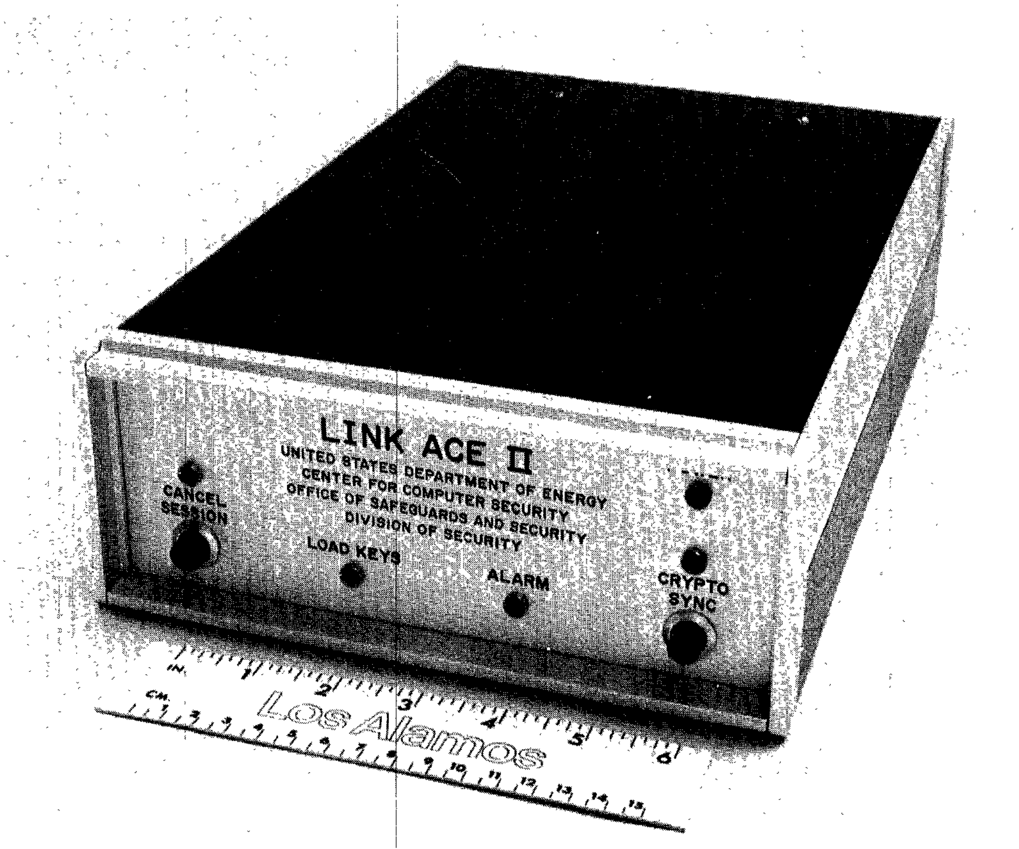
LINK ACE II
UNITED STATES DEPARTMENT OF ENERGY
CENTER FOR COMPUTER SECURITY
OFFICE OF SAFEGUARDS AND SECURITY
DIVISION OF SECURITY
CANCEL SESSION
LOAD KEYS
ALARM
CRYPTO SYNC
Los Alamos

Fig. 1. The Link Access Control and Encryption (ACE) II provides protection for unclassified sensitive data transmission between central computers and remote terminals.

The CCS provided measurements of the isolation between channels on this LAN. We coordinated the performance of these measurements using a team of experts from the Electronics, Operational Security, and Energy Divisions of the Los Alamos National Laboratory. The testing considered receiver sensitivity and bandwidth, LAN-signal operating levels, the intermodulation distortion products that appear as crosstalk between channels, and the effect of abnormal operating conditions on the isolation between channels.

We expect these measurements to provide a sound technical basis for evaluating the practicality of providing data communication services for more than one level of data processing (for example, classified, private, administrative) on a single LAN while maintaining adequate security for the sensitive data. Several DOE sites are installing or using broadband

LANs. Development of appropriate test procedures and criteria should provide a model for other sites to use in evaluating security performance of LANs.

V. SPECIAL PROJECTS

A. WBCN Support

1. WBCN Security Committee Subtask. The Office of Military Applications (OMA) has initiated a major program to implement modern methods of design and manufacturing by using the latest computer-integrated manufacturing techniques. OMA has directed the DOE Nuclear Weapons Complex design agencies and manufacturing facilities to electronically conduct all interactions and document transfers associated with the development of the Trident II. In response to the directive, a group of representatives from various DOE and DOE contractor facilities has been formed to link the necessary facilities involved in the Trident II effort. This network is named the Wide-Band Communications Network (WBCN). Center personnel have been active in this group from its beginning.

2. Document Phase II Security Requirements. A member of the Center chaired the group that wrote the Master Security Plan and the Site Security-Plan Outline and revised the Security Requirements for Phases I and II. To achieve the necessary concensus document, drafts were prepared and circulated. Modifications were incorporated into the second drafts, and the drafts again circulated until a consensus document was achieved. The final reports were approved and issued. The documents for Phase III are now going through the same process.

3. Common-Time Module. Because management must be able to correlate network events that have security or operational significance, the Center is developing a common-time module that ensures that each WBCN gateway can access an accurate clock. The equipment being tested derives the time from the NBS standard time using Radio Station WWV frequency transmissions.

4. DEC Software. The WBCN Data Encryption Standard (DES) software suite including encryption, key distribution, key management, and supporting software is installed and running on the Los Alamos WBCN gateway, operated by Los Alamos group C-5. The NSA-supplied DES keying material has been received and installed on the gateway. Software documentation, preparation of a users' manual, and operator training are proceeding.

5. Test Bed. To support the DOE in its efforts to develop a data communication network to electronically conduct interactions and transfers of documents throughout the DOE Nuclear Weapons Complex, a computer systems and communications circuits system has been installed at the Center. Because both the Nuclear Weapons Complex WBCN and the DOE Telecommunications Operational Model (OPMODEL) satellite communications project, Phase I, have selected Digital Equipment Corporation (DEC) computer hardware and software products, the WBSTB has been developed using the same products. The WBSTB as originally defined consists of two DEC VAX 11/730 computers, each equipped with two communications interfaces and interconnected with a full-duplex, simulated communications circuit. This arrangement emulates either a pair of network gateways on a wide-bandwidth network or one gateway and an attached, local computer. An additional VAX 11/730, obtained through the DOE excess property list, provides the ability to emulate a computer connected to a wide-band network through the two 11/730 gateways.

The construction of a DOE/CCS computer laboratory located in Building 114 and the installation of the WBSTB hardware were completed. The new computer facility (Fig. 2) consists of power and air-conditioning equipment, has a raised floor and wireways, and provides a physical layout and environment consistent with modern computer standards. The installation of operating systems VAX/VMS version 4.1, DECnet networking software, and FORTRAN 77 and C programming language software was completed.

B. SPARTA Contract

The Center has contracted with SPARTA to provide support for WBCN security testing. This work will ensure that the security features of the network achieve their goals; that the physical, personnel, and communications security assumptions are documented; and that the analysis and report will pertain to the WBCN gateway computers.

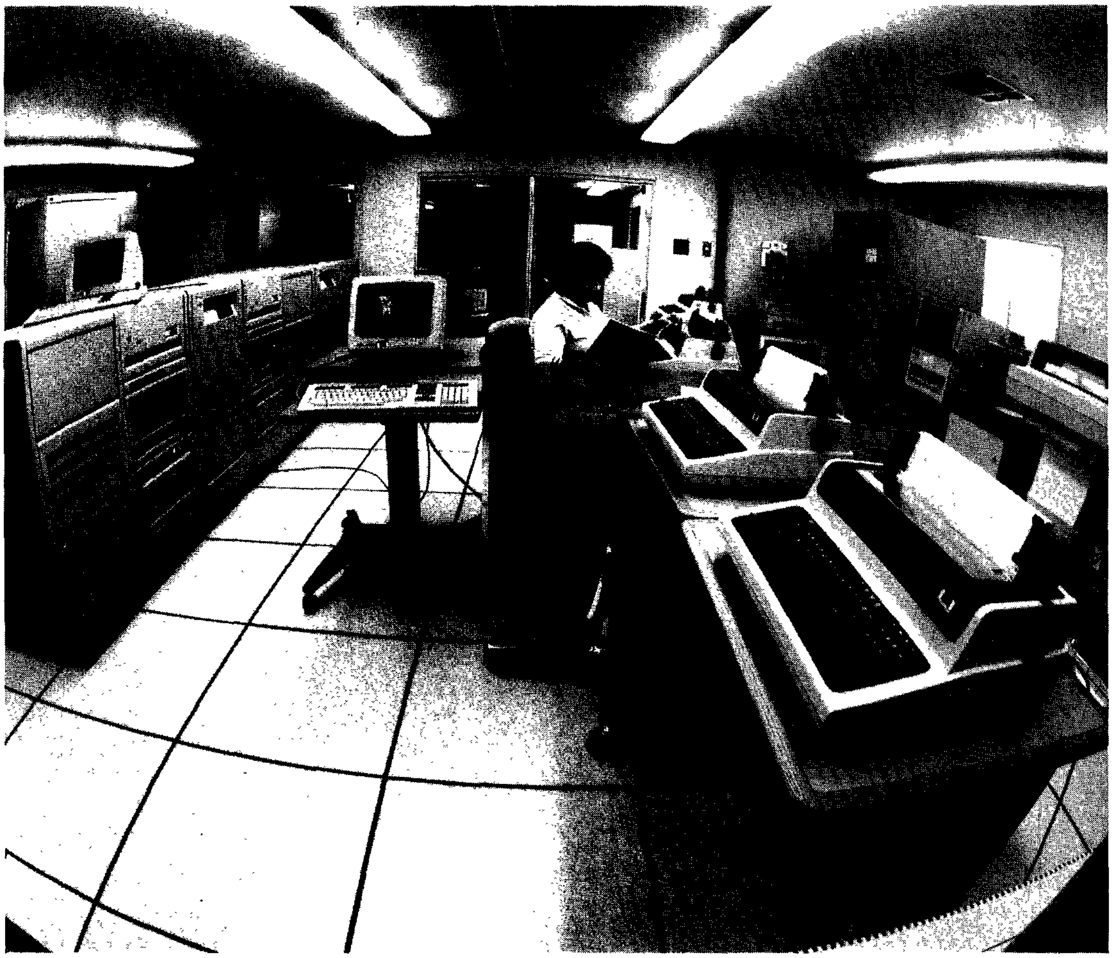

Fig. 2. The Center's computer laboratory houses the Wide Band Security Test Bed and provides a physical layout and environment consistent with modern computer standards.

VI. DOE HEADQUARTERS DIRECTED ASSISTANCE

A. DOE/NCSC Council

Center personnel participated in quarterly meetings of the DOE/NCSC Council. We presented the DOE Center research and development plans to the Council, and Center personnel were represented on two working groups, Secure Networks and Training.

B. I&E Support

At the request of the DOE Office of Safeguards and Security (DOE/OSS), the Center provided assistance to the Inspection and Evaluation (I&E) Standards and Criteria Computer Security Working Group. Center members chaired the continuity of operations working group and the ratings working group and participated in the general committee meetings. The continuity of operations working group drafted a report and submitted it to the DOE/OSS for review. In revisions to the draft, citations from applicable DOE Orders were added to all Standards addressed by current DOE policy. The group also drafted suggestions for policies for Standards that are not covered by DOE Orders.

VII. EXPLORATORY RESEARCH AND DEVELOPMENT

Inspection of electronic data processing (EDP) equipment and associated hardware to detect unauthorized modification includes transportation of the suspect equipment to an inspection facility, disassembly of the equipment, and x-ray or radiography of suspected components. The cost associated with these activities can be great, for example, the cost of transporting the equipment from a foreign country to a facility in the U.S. or the loss of use of the equipment. To address this cost problem, we are investigating the following areas:

- Are there automated means of detecting unauthorized modification of EDP equipment?
- Are there unique "signatures" associated with EDP components, which can be used as standards for future comparisons?
- Are there automated means to detect the presence of chip-level substitution, addition, or modification?
- Is it possible to detect unauthorized modification of software?

The approach to this potential research program is to develop a variety of detection devices ranging from portable devices with low- to intermediate-level detection capabilities for <u>in situ</u> testing to devices with very high detection capabilities for testing laboratory-based critical components. Several promising techniques consistent with this philosophy have been identified and include methods based on acoustical, electromagnetic, and optical phenomena.

Digital imaging techniques can be used to collect, enhance, analyze, and present data originating from acoustical, electromagnetic, and optical phenomena. We conducted preliminary experiments with a charge-coupled device camera to image "before" and "after" situations to detect chip-level modification of a printed circuit board. The results clearly show that such modification can be detected easily. We are also considering holographic interferometry as a tool. Early results suggest that this method could provide very high detection capabilities. Current activities include infrared imaging and further work on image-processing software.

Printed in the United States of America
Available from
National Technical Information Service
US Department of Commerce
5285 Port Royal Road
Springfield, VA 22161

Microfiche (A01)

	NTIS		NTIS		NTIS		NTIS
Page Range	Price Code	Page Range	Price Code	Page Range	Price Code	Page Range	Price Code
001-025	A02	151-175	A08	301-325	A14	451-475	A20
026-050	A03	176-200	A09	326-350	A15	476-500	A21
051-075	A04	201-225	A10	351-375	A16	501-525	A22
076-100	A05	226-250	A11	376-400	A17	526-550	A23
101-125	A06	251-275	A12	401-425	A18	551-575	A24
126-150	A07	276-300	A13	426-450	A19	576-600	A25
						601-up*	A99

*Contact NTIS for a price quote.